## 契約課発行の文書に署名された電子署名を 電子証明書の取り込みによって検証する方法

1, ダウンロードした「certificate.fdf」をダブルクリックする。



Adobe Reader が起動し、下掲のダイアログが表示されます。
 「連絡先の信頼を設定」をクリックしてください。

データ交換ファイル - 連絡先を取り込み
次のデータが含まれている FDF データ交換ファイルを開きました : 連絡先 - 送信者
名前: 越谷市権限者 電子メールアドレス: 10031300@city.koshigaya.saitama.jp
信頼済み証明書の一覧に証明を追加 このファイルには、越谷市権限者の連絡先が含まれています。この連絡先をどのように「信頼済み証 明書」の一覧に含めるかのオプションを設定するには、「連絡先の信頼を設定」をクリックします。連絡 先情報に含まれている証明書は、いったん信頼すると、それを使用して関連する連絡先の署名を検 証したり、その連絡先宛ての文書を暗号化することができます。
連絡先の信頼を設定(丁) 閉じる( <u>C</u> )

3,「連絡先設定を取り込み」のダイアログが出ますので、「証明書の詳細」をクリックして 証明書の情報を表示させてください。

連絡先設定を取り込み
サブタイトル: 越谷市権限者
発行者: LGPKI
使用方法: 署名処理,文書に署名
有効期限: 2011.10.03 01:55:58 Z
「信頼」ポリシーの制限
2次の対象についてこの意形明書を信頼します:
「 <b>署</b> 名、および注頼されたルート(R)
□ 証明済み文書(I)
□ダイナミックコンテンツ(D)
□ 埋め込まれている特権の高い JavaScript(」)
[III]目書の詳細(E)
ヘルプ OK キャンセル

4,「証明書ビューア」が立ち上がるので、「詳細」タブをクリックしてください。

証明書ビューア	$\mathbf{X}$
このダイアログボックスを使用して れる詳細は、選択したエントリにさ の発行チェーンが表示されていま	、証明書およびその発行チェーン全体の詳細を表示できます。表示さ 対応しています。信頼点によって発行されたチェーンがないため、複動 す。 示( <u>5</u> )
□ LGPKI 越谷市権限者	概要 詳細 失効 信頼 ポリシー 法律上の注意事項
	越谷市権限者 (The Digital Authentication 地方公共団体 (Local Governments)         発行者:       LGPKI
	有効期間の開始: 2008/10/03 10:55:59 +09'00'
	4 の使用方法: 署名処理, 文書に署名
	,
<ul> <li>選択した証明書パスは有効</li> </ul>	<u>िवटळ000</u>
パスの検証は 2008/10/06 1 検証モデル : シェル	.0:55:21 +09'00' に行われました
	ОК

5,「詳細」タブに「証明書」の詳細な情報が記載されております。 手順に従い、越谷市の証明書であることを確認してください。

証明書ビューア		×
このダイアログボックスを使用して れる詳細は、選択したエントリにす の発行チェーンが表示されていま	、証明書およびその発行チェーン全体の詳細を表示できます。 対応しています。信頼点によって発行されたチェーンがないため、 す。 示(5)	表示さ 、複数
■ LGPKI 越谷市権限者	概要 詳細 失効 信頼 ポリシー 法律上の注意事: 証明書データ(D):	項
	名前       値	
③ 選択した証明書パスは有効 パスの検証は 2008/10/06 1 検証モデル:シェル	)です。 10:55:21 +09'00' (ご行われました	
		K

6,「サブジェクト」を選択して、内容を確認してください。

cn=The Digital Authentication Authorities of Koshigaya City ou=Contracting Section ou=General Affairs Department ou=Koshigaya City l=Saitama o=Local Governments c=JP

## 証明書ビューア

## このダイアログボックスを使用して、証明書およびその発行チェーン全体の詳細を表示できます。表示さ れる詳細は、選択したエントリに対応しています。信頼点によって発行されたチェーンがないため、複数 の発行チェーンが表示されています。

×

☑ 見つかったすべての証明パスを表示(5)

■ LGPKI 越谷市権限者	一概要  ■	≠#Ⅲ <u>矢効</u> データ( <u>D</u> ):	1言頼    ボリシー	・   法律上の注意事	刵
		名前	値		^
	📄 /	ドージョン	3		=
		署名アルゴリ	SHA1 RSA		
		ナブジェクト	cn=The Digital	Authentication	
	63	能行者	ou=Organizatio	on CA U8, o=LG	
		リアル番号	31 35 31 35 38		
		自効期間の	2008/10/03 10	:55:59 +09'00'	
		月初期間の…	2011/10/03 10	:55:58 +09'00'	<u>×</u>
	c=JP				
違択した証明書パスは有 パスの検証は 2008/10/06 検証モデル:シェル	効です。 5 10:55:21 +09	'00' に行われまし	た		
					ок

7,「発行者」を選択して、内容を確認してください。

ou=Organization CA U8 o=LGPKI

c=JP

このタイアログボックスを使用して、証明書およびその発行チェーン全体の詳細を表示できます。表示される詳細は、滋知したエントリに対応しています。信頼点によって発行されたチェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、准数の発行チェーンがないため、体数の発行チェーンがないため、体数の発行チェーンがないため、体数の発行チェーンがないため、体数の発行チェーンがないため、体数の発行チェーンが表示されています。 <ul> <li></li></ul>	証明書ビューア	
<ul> <li>□ LGPKI</li></ul>	このダイアログボックスを使用して、 れる詳細は、選択したエントリにま の発行チェーンが表示されていま	、証明書およびその発行チェーン全体の詳細を表示できます。表示さ す応しています。信頼点によって発行されたチェーンがないため、複数 す。 示(5)
名前       値         パージョン       3         富       パージョン       3         富       若名アルゴリ       SHA1 RSA         同       サブジェクト       cn=The Digital Authentication         ご       第行者       ou=Organization CA U8, o=LG         回       シリアル番号       31 35 31 35 38         回       有効期間の       2008/10/03 10:55:59 +09'00'         回       有効期間の       2011/10/03 10:55:58 +09'00'         回       ローOrganization CA U8         o=LGPKI       c=JP         OU=Organization CA U8       o=LGPKI         c=JP       U         Warlow Expendence       X2.0枚設計         変択した証明書パスは有効です。       パスの検証は 2008/10/06 10:555:21 +09'00' に行われました         検証モデル: シェル       シェル	■ LGPKI 越谷市権限者	概要 詳細 失効 信頼 ポリシー 法律上の注意事項 証明書データ(D):
<ul> <li>         譲択した証明書パスは有効です。         パスの検証は 2008/10/06 10:55:21 +09'00' に行われました         検証モデル: シェル     </li> </ul>		<ul> <li>名前 値</li> <li>○ バージョン 3</li> <li>○ 署名アルゴリ SHA1 RSA</li> <li>○ サブジェクト cn=The Digital Authentication</li> <li>○ 発行者 ou=Organization CA U8, o=LG</li> <li>○ シリアル番号 31 35 31 35 38</li> <li>○ 有効期間の 2008/10/03 10:55:59 +09'00'</li> <li>○ 有効期間の 2011/10/03 10:55:58 +09'00'</li> </ul>
	選択した証明書パスは有効 パスの検証は 2008/10/06 1 検証モデル:シェル	です。 0:55:21 +09'00' に行われました

8,「シリアル番号」を選択して、内容を確認してください。

31 35 31 35 38

証明書ビューア		
このダイアログボックスを使用して、 れる詳細は、選択したエントリにえ の発行チェーンが表示されていま	、証明書およびその発行チェーン全体の詳細を表示できます。 す応しています。信頼点によって発行されたチェーンがないため、 す。 示(5)	表示さ 複数
■ LGPKI 越谷市権限者	概要 詳細 失効 信頼 ポリシー 法律上の注意事功 証明書データ(D):	۹ 
	名前       値         戸/「ジョン 3       3         冨 邦ブジェクト       cn=The Digital Authentication ou=Organization CA U8, o=LG         愛行者       0u=Organization CA U8, o=LG         ジリアル番号       31 35 31 35 38         同       有効期間の       2008/10/03 10:55:59 +09'00'         同       有効期間の       2011/10/03 10:55:58 +09'00'         31 35 31 35 38       31 35 31 35 38	
③ 選択した証明書パスは有効 パスの検証は 2008/10/06 1 検証モデル:シェル	です。 0:55:21 +09'00' (ご行われました の*	<

9, SHA1ダイジェストを選択して、内容を確認してください。

## EC AE 83 48 45 6A 2D 5B 2B CB 68 F7 8B D7 13 A8 BA 97 45 01

証明書ビューア		×
このダイアログボックスを使用して、 れる詳細は、選択したエントリに対 の発行チェーンが表示されています	証明書およびその発行チェーン全体の詳細を表示できます。 打応しています。信頼点によって発行されたチェーンがないため す。 示(S)	表示さ 、複数
<ul> <li>□ LGPKI</li> <li>越谷市権限者</li> </ul>	概要 詳細 失効 信頼 ポリシー 法律上の注意事 証明書データ(D):	Щ
	名前       値 <ul> <li>●</li> </ul> <li>●</li>	5
③ 選択した証明書パスは有効で	ट्वं.	
パスの検証は 2008/10/06 10 検証モデル:シェル	0:55:21 +09'00' に行われました	
		ж

10,以上 4 つの証明書情報がすべて合致すれば、その証明書は越谷市のものです。以上で 証明書の検証は完了です。「OK」を押してください。証明書の取り込み及び信頼の手順に 進みます。 11,「連絡先設定を取り込み」ダイアログに戻りますので、「署名、および信頼されたルート」、「証明済み文書」の2つの項目のチェックボックスにチェックを入れてください。 これで越谷市の証明書を前述の2項目において信頼するという設定が完了です。「OK」 をクリックして証明書をAcrobat Reader に取り込んでください。

連絡先設定を取り込み
証明書の詳細 サブタイトル: 越谷市権限者 発行者: LGPKT
使用方法:署名処理,文書に署名
有効期限: 2011.10.03 01:55:58 Z 信頼 ポリシーの制限
<ul> <li>次の対象についてこの証明書を信頼します:</li> <li>■ 署名、および信頼されたルート(№)</li> <li>● 証明済み文書(T)</li> <li>■ ダイナミックコンテンツ(D)</li> <li>■ 埋め込まれている特権の高い JavaScript(J)</li> </ul>
証明書の詳細(E)
ヘルプ OK キャンセル

12,「取り込みの終了」ダイアログが表示されたら、「証明書」の取り込みは完了です。

取り込みの終了
取り込みの詳細:
連絡先「越谷市権限者」の取り込み:成功しました。 1 個の証明書が取り込まれ、「越谷市権限者」に追加されまし;
К

13, 次から契約課から発行された電子署名の付与された文書を開くと、その電子署名の検 証を行うことができます。

※このマニュアルは Adobe Reader 8 用となりますが、Adobe Reader のその他のバージョ ンでも、証明書の取り込み方法はほぼ同じです。